IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN RE: MARRIOTT INTERNATIONAL, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	MDL No. 19-md-2879 Judge Paul W. Grimm
This Document Relates To: DENNIS MCGRATH, Individually and on behalf of all others similarly situated, Plaintiff, vs. MARRIOTT INTERNATIONAL, INC., ARNE M. SORENSON, KATHLEEN KELLY OBERG, BAO GIANG VAL BAUDUIN, BRUCE HOFFMEISTER, MARY K. BUSH, FREDERICK A. HENDERSON, LAWRENCE W. KELLNER AYLWIN B. LEWIS, and GEORGE MUÑOZ Defendants.	This document relates to Case No. 8:19-cv-00368-PWG

MEMORANDUM IN SUPPORT OF DEFENDANTS' MOTION
TO DISMISS THE THIRD AMENDED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

TABLE OF CONTENTS *(continued)*

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES *(continued)*

Page(s)

TABLE OF AUTHORITIES *(continued)*

Page(s)

TABLE OF AUTHORITIES *(continued)*

Page(s)

TABLE OF AUTHORITIES *(continued)*

Page(s)

Statutes

Regulations

Legislative Materials

TABLE OF AUTHORITIES *(continued)*

Page(s)

Other Authorities

Defendants respectfully move, under the Private Securities Litigation Reform Act of 1995 ("PSLRA"), and Rules 12(b)(6) and 9(b) of the Federal Rules of Civil Procedure, to dismiss the Third Amended Consolidated Class Action Complaint ("Complaint") with prejudice.

INTRODUCTION

In 2016, Marriott International, Inc. ("Marriott" or the "Company") acquired Starwood Hotels and Resorts Worldwide, LLC ("Starwood"). On November 30, 2018, Marriott announced a data security incident involving Starwood's guest reservation database. The next day, an investor filed the first suit claiming that the ensuing dip in the Company's stock price revealed that Marriott had defrauded its shareholders.

Plaintiff's claims fail as a matter of law. In 1995, Congress enacted the PSLRA to curb abusive securities suits filed reflexively, and without credible evidence of fraud, when companies' stock prices declined. The PSLRA requires plaintiffs to allege with factual particularity which statements they claim are misleading and why. 15 U.S.C. § 78u–4(b)(1). It also requires them to plead a "strong inference" that the defendants perpetrated "each act or omission alleged" with scienter, i.e., a culpable state of mind embracing intentional or reckless deceit on investors. *Id.* § 78u–4(b)(2)(A). This unique pleading standard does not draw all inferences in favor of plaintiffs, but rather requires courts to balance the competing inferences of scienter and innocence. *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 324 (2007). Securities fraud claims can survive dismissal "only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any opposing inference." *Id.* The Complaint does not satisfy these burdens.

First, the Complaint fails to plead any misstatement. What investors learned on November 30, 2018 is that Marriott—like every other company in the world—is susceptible to cyberattacks. Defendants never said otherwise. And it would be absurd for anyone to assume otherwise, especially given that Marriott repeatedly cautioned investors that "[c]yber-attacks could

have a disruptive effect on [its] business." ¶¶ 460, 485, 494, 505, 515, 522, 530, 539, 553, 560, 567, 587.[1]

Plaintiff strains to portray the discovery of the data security incident as being inconsistent with various statements about Marriott's acquisition of Starwood, but it is not. For example, the Complaint maligns Defendants for expressing optimism about the acquisition, and for commenting on their due diligence and integration efforts. None of those statements, however, represented that Marriott had extinguished all risks it undertook in the transaction, much less cybersecurity risks in particular. And there is nothing inconsistent between being optimistic about a groundbreaking acquisition and the discovery later that criminals had secretly attacked Starwood. Thus, the Complaint is left to vacillate between speculation that Marriott's due diligence was so detailed that it must have uncovered problems and so cursory that mere references to Marriott's diligence efforts must have been false. None of these conflicting accounts of the facts pleads any false statements.

Because Defendants never said anything misleading, the Complaint resorts to criticizing what they did not say. This tactic—the last bastion of every litigant who seeks recovery for a fraud it cannot name—also fails. Omission liability arises under the PSLRA only when a plaintiff specifically pleads that a defendant "omitted to state a material fact necessary in order to make [its] statements made . . . not misleading." 15 U.S.C. § 78u–4(b)(1)(B). In other words, Defendants can be liable for omissions only when they have made affirmative statements that are deceptively incomplete. Plaintiff fails to identify any such affirmative statements. Thus, its theory that Marriott was required to announce various security vulnerabilities—which may well have invited criminal attacks—has no firmer footing in the law than it has in common sense.

[1] All references herein to "¶ ___" are citations to the Complaint.

Second, the Complaint fails to allege that Defendants spoke with scienter. There is not a single allegation that supports the inference that Defendants intended to trick investors into believing that Marriott was impervious to cyberattacks or spoke with reckless disregard for whether investors would draw that conclusion. Instead, the Complaint expends more than 300 pages criticizing Marriott's cybersecurity measures. These criticisms are irrelevant in light of Defendants' statements. The securities laws do not regulate cybersecurity; they regulate candor in the sale of securities. The protracted maze of allegations Plaintiff weaves for the Court to untangle addresses only the former and, thus, cannot support an inference of scienter.

On the other hand, the Complaint is replete with allegations that support inferences of innocence. It admits Marriott hired experts to launch an investigation within two days of detecting suspicious activity in the guest reservations database. ¶ 32. It admits Marriott promptly alerted the FBI, ¶ 35—which a fraudster would not conceivably have done if it meant uncovering a scheme to defraud investors. It admits Marriott "began preparations to notify affected guests" on the same day it learned that files containing their information may have been exposed. ¶ 259. And it fails to plead that Defendants had anything to gain by misleading investors. Viewed holistically, the inferences that Defendants acted innocently eclipse any possible inference of scienter.

Not surprisingly, virtually every court that has considered securities claims based on a data breach has rejected them. The sole exception—*In re Equifax Inc. Securities Litigation*, 357 F. Supp. 3d 1189 (N.D. Ga. 2019)—is most notable because it rejected many of the same arguments Plaintiff presses and permitted limited claims to proceed only because the defendant expressly touted "advanced security protections" it knew it did not have. *Id*. at 1219–20. The absence of any similar misrepresentation here illustrates why this case must be dismissed, almost as powerfully as the string of rulings dismissing more analogous claims. *See infra* at 8–9.

Plaintiff's attempt to harvest securities fraud claims from a cyberattack arrives at a critical juncture when cyberattacks are becoming increasingly inevitable. As former FBI Director Robert Mueller observed, "there are only two types of companies: those that have been hacked and those that will be," and "they are converging into one category: companies that have been hacked and will be hacked again."[2] Subjecting cyberattack victims, who never promised invulnerability to such crimes, to the added burden of securities class actions would fuel the rise of such collateral litigation in the wake of every cyberattack, in contravention of the letter and intent of the PSLRA.

This lawsuit should be dismissed with prejudice.

SUMMARY OF THE ALLEGATIONS

I. THE PARTIES.

Founded in 1927, Marriott is one of the largest and most respected hospitality companies in the world. Marriott operates, franchises, and licenses hotel, residential, and timeshare properties across the globe. Marriott is incorporated in Delaware and headquartered in Maryland. ¶ 50.

Four of the individual Defendants are officers of Marriott. Mr. Sorenson has served as the Company's President since May 2009, a member of its Board of Directors since 2011, and its Chief Executive Officer since March 2012. ¶ 51. Ms. Oberg has served as the Chief Financial Officer since 2016. ¶ 52. Mr. Bauduin has served as the Chief Accounting Officer since 2014. ¶ 53. Mr. Hoffmeister served as the Chief Information Officer since 2011 (but recently retired). ¶ 54.

The remaining Defendants, Ms. Bush and Messrs. Henderson, Kellner, Muñoz, and Lewis are not employees, but each served on Marriott's Board of Directors and its Audit Committee during some or all of the relevant time. ¶¶ 58–62.

[2] Robert S. Mueller III, Director, Fed. Bureau of Investigation, Remarks at the RSA Cyber Security Conference (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

The Court appointed the Construction Laborers Pension Trust for Southern California as Lead Plaintiff ("Plaintiff") for this litigation, referred to in the broader MDL proceedings as the "Securities Track." Plaintiff is a pension plan that allegedly acquired Marriott stock. ¶ 49.

II. THE STARWOOD ACQUISITION.

Over the past decade, Marriott has grown its business successfully by acquiring and integrating other hospitality companies. ¶¶ 112–14. In 2015, Marriott determined that acquiring Starwood would "grow[] value for shareholders" by "driv[ing] revenue growth" and allowing Marriott to "gain market share." ¶¶ 120, 442. On November 16, 2015, Marriott announced its plan to acquire Starwood (the "Acquisition"). ¶ 122. Industry analysts remarked on the potential of "a global lodging powerhouse with more rooms than anyone in the world." ¶ 130. Among other benefits, analysts noted the significant "revenue synergy opportunities," ¶ 132; "[c]ombined marketing and sales strategies," ¶ 133; "access to a more diverse client base," *id.*; "increased brand loyalty," *id.*; and a "combined rewards program," ¶ 134. Marriott and analysts viewed Starwood's customer loyalty program as an important asset, ¶¶ 6, 132, but that program is different from the "reservation database" that hackers accessed in the data security incident (despite Plaintiff's confusion of the two in calling the database a "focal point[]" of the Acquisition, ¶ 7).

Marriott devoted extensive resources to due diligence and integration planning in connection with the Acquisition. ¶¶ 146–47. Marriott periodically issued updates on those efforts. ¶¶ 142–47. Plaintiff does not allege that Marriott made any specific disclosures about due diligence on cybersecurity, but that is not to say that Marriott conducted none. As the Complaint acknowledges, Marriott devoted significant resources to such diligence. *See, e.g.*, ¶¶ 175–76 (describing Marriott's IT-specific due diligence process as "extremely detailed").

The market was under no illusion that creating "the largest hotel company in the world," ¶ 2, would be a quick or simple process. Marriott was forthright about the "challenges" of "integrating the two companies." ¶¶ 442, 452. After the Acquisition, Marriott provided occasional updates regarding its progress on integrating Starwood. *E.g.*, ¶¶ 526, 543. None of these statements addressed Starwood's IT systems, guaranteed those systems were invulnerable to cyberattacks, or represented they could be easily merged with Marriott's systems. In fact, Marriott's SEC filings disclosed that "[c]yber-attacks could have a disruptive effect on our business," and that there may be difficulty "harmonizing our different reservations and other systems." *E.g.*, ¶¶ 528, 530.

III. THE CRIMINAL CYBERATTACK ON THE COMPANY.

On September 7, 2018, IBM Guardium, a security product used on Starwood's systems, generated an alert that an unknown user had run a query in the Starwood guest reservation database. ¶ 32. "Accenture, Marriott's third party IT contractor tasked with running the legacy Starwood guest reservation database, alerted Marriott[] the following day," and "Marriott brought in third-party investigators . . . to perform a review of their hacked systems" two days later. *Id.* On September 17, 2018, the investigators uncovered malware that could be used to access or monitor a computer. ¶ 256. Mr. Sorenson informed the Board the next day. *Id*.

On November 13, 2018, the third-party investigators discovered that two encrypted files had been deleted from a device they were examining. ¶ 259. On November 19, 2018, the investigators discovered that the files contained customers' personal information. *Id.* That very same day, Marriott began preparing to notify affected guests. *Id.*

On November 30, 2018, Marriott publicly announced the data security incident. ¶ 262. The Company's stock price declined from its prior closing price of $121.84 to $115.03 per share on the day of the announcement. ¶ 39. By the next day of trading, Marriott's stock price recovered more

than 70% of these losses, closing at $119.53. Over the following year, Marriott's stock price increased by 17.5%, closing above its pre-announcement price at $140.43 on December 2, 2019.[3]

IV. THE CLAIMS.

On December 1, 2018, one day after Marriott announced the data security incident, a litigant filed the first putative securities class action. *See McGrath v. Marriott Int'l, Inc.*, No. 18-6845 (E.D.N.Y. Dec. 1, 2018). The Judicial Panel on Multidistrict Litigation transferred that lawsuit to this Court, along with consumer lawsuits filed after the Company's announcement.

On July 24, 2020, Plaintiff filed the third amended complaint. ECF No. 609.[4] Seeking to sue on behalf of a class of investors, ¶ 650, Plaintiff claims that Defendants made misleading statements or omissions from November 16, 2015 to November 29, 2018 (the "Class Period") regarding the Company's commitment to protecting customer data, its due diligence and integration efforts for the Acquisition, and its cybersecurity risks. Spanning 317 pages, the Complaint is replete with allegations copied from parallel lawsuits; relies heavily on a forensic report (the "PFI Report") issued almost six months after the Class Period; and recites opinions from seven confidential witnesses ("CWs") about the strength of Marriott's (or Starwood's) cybersecurity measures. It disputes every periodic report Marriott filed with the SEC, every filing regarding the Acquisition, and numerous other statements made throughout the Class Period. *See* ¶¶ 442–587. It pleads no specific allegations, however, controverting the truth those statements at the time they were made, or addressing Defendants' beliefs or intentions regarding their communications with investors.

---

[3] Yahoo! Finance, Marriott Int'l, Inc., https://finance.yahoo.com/quote/MAR/history?period1=1543276800&period2=1575331200&interval=1d&filter=history&frequency=1d (last visited Sept. 8, 2020). In considering this motion to dismiss, the Court "may take judicial notice of published stock prices," *Greenhouse v. MCG Capital Corp.*, 392 F.3d 650, 655 n.4 (4th Cir. 2004), and "is entitled to rely on public documents quoted by, relied upon, incorporated by reference or otherwise integral to the complaint," *In re Royal Ahold N.V. Sec. & ERISA Litig.*, 351 F. Supp. 2d 334, 349 (D. Md. 2004) (quotation marks and citation omitted).

[4] All ECF references herein are to the consolidated multidistrict litigation docket, MDL No. 19-md-2879.

ARGUMENT

The Complaint must be dismissed. Count I is a claim for securities fraud under Section 10(b) of the Securities Exchange Act of 1934 and SEC Rule 10b–5 promulgated thereunder. ¶¶ 656–63. To state a claim, a plaintiff must allege: (1) a material misrepresentation or omission; (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance on the misrepresentation or omission; (5) economic loss; and (6) loss causation. *Yates v. Mun. Mortg. & Equity, LLC*, 744 F.3d 874, 884 (4th Cir. 2014). The Complaint's failure to plead any material misstatement or omission, scienter, or loss causation dooms Count I.

Count II asserts claims under Section 20(a) of the Exchange Act, which imposes secondary liability on persons who control primary violators. *See* ¶¶ 664–72. Count II fails because the Complaint pleads no primary violation.

A tide of rulings in analogous cases illustrates the deficiencies of this case. For example, after Heartland Payments Systems suffered a cyberattack exposing 130 million payment card numbers, shareholders accused the company of misrepresenting its data security practices. *In re Heartland Payment Sys., Inc. Sec. Litig.*, 2009 WL 4798148 (D.N.J. Dec. 7, 2009). The court dismissed the claims, holding that "suffer[ing] a security breach does not demonstrate that the company did not 'place significant emphasis on maintaining a high level of security,'" particularly where its SEC filings "ma[d]e clear that Heartland was not claiming its security system was invulnerable." *Id.* at *5. The court held that the plaintiffs failed to plead scienter, notwithstanding "after-the-fact speculation by a handful of lower-level employees . . . that Heartland was not paying proper attention to its security problems," *id.* at *7–8. The same reasoning applies here.

Equifax stands alone as the only case that has even partially denied dismissal of securities claims premised on a cyberattack, and it did so based on incomparable facts: the defendant falsely

promoted to investors its "intrusion testing, vulnerability assessments, on-site inspections" and "rigorous enterprise risk management program that targeted its cybersecurity risks." 357 F. Supp. 3d at 1221–22. Plaintiff's failure to plead any similar representations confirms that this case fails even under *Equifax*'s reasoning. And all other securities fraud suits based on various types of data security incidents have been dismissed for reasons similar to those that compel dismissal here.[5]

I. THE PSLRA IMPOSES UNIQUE AND EXACTING PLEADING STANDARDS.

Prior to the enactment of the PSLRA, private securities fraud actions were "employed abusively to impose substantial costs on companies . . . whose conduct conform[ed] to the law." *Tellabs*, 551 U.S. at 313 (citation omitted). Litigants would await negative news stories or stock drops and then reflexively file boilerplate complaints, hoping that wrongdoing would be uncovered through discovery or that the cost of discovery itself would coerce companies into settlement. *See, e.g.*, *Cozzarelli v. Inspire Pharms. Inc.*, 549 F.3d 618, 623 (4th Cir. 2008). The PSLRA was enacted with bipartisan support to curb such abusive litigation. H.R. Rep. No. 104-369, at 31, 33, *as reprinted in* 1995 U.S.C.C.A.N. 730, 730, 732 (Conf. Rep.).

"Congress charged courts to be vigilant in preventing meritless securities fraud claims from reaching the discovery phase of litigation." *Cozzarelli*, 549 F.3d at 623; *see Pub. Emps.' Ret. Ass'n of Colo. v. Deloitte & Touche LLP*, 551 F.3d 305, 311 (4th Cir. 2009). "[T]he PSLRA installed both substantive and procedural controls." *Tellabs*, 551 U.S. at 320 (quotation marks and citations

[5] *See In re Alphabet, Inc. Sec. Litig.*, 2020 WL 2564635, at *4 (N.D. Cal. Feb. 5, 2020) (dismissing § 10(b) claim; non-disclosure of vulnerability did not render risk disclosures or "commitment" to protecting data misleading); *In re Facebook, Inc. Sec. Litig.*, 2020 WL 4569443 (N.D. Cal. Aug. 7, 2020) (dismissing § 10(b) claim; risk disclosures, responses to data misuse, and assurances of GDPR-compliance were not actionable); *Sgarlata v. PayPal Holdings, Inc.*, 409 F. Supp. 3d 846 (N.D. Cal. 2019) (dismissing § 10(b) claim for failing to plead that defendants knew scope of breach of 1.6 million customers' data); *In re Intel Corp. Sec. Litig.*, 2019 WL 1427660, at *11 (N.D. Cal. Mar. 29, 2019) (dismissing § 10(b) claim; promoting "security" of Intel processors without disclosing vulnerabilities "did not create a false impression" or mislead "reasonable investors" about potential security threats); *In re Qudian Inc. Sec. Litig.*, 2019 WL 4735376, at *8 (S.D.N.Y. Sept. 27, 2019) (dismissing §§ 11, 12, 15 claims; omitting past data breach did not render statements about "sophisticated security protocols" misleading where company disclosed that its "far from perfect" security systems "might have been breached in the past").

omitted). One such control is "[e]xacting pleading requirements." *Cozzarelli*, 549 F.3d at 623 (quoting *Tellabs*, 551 U.S. at 313). These standards are discussed further below.

II. THE COMPLAINT FAILS TO PLEAD A MISSTATEMENT OR OMISSION.

To state a claim under Section 10(b) and Rule 10b–5, Plaintiff must allege either (a) an untrue statement of material fact or (b) the omission of a material fact that was necessary to make a particular statement not misleading in light of the circumstances in which it was made. 15 U.S.C. § 78u–4(b)(1). The PSLRA requires plaintiffs to "specify each [allegedly misleading] statement" and "the reason or reasons why the statement is misleading." *Tellabs*, 551 U.S. at 321 (2007). "Plaintiffs asserting claims under Rule 10b–5 must do more than say that the statements . . . were false and misleading: they must demonstrate with specificity why and how that is so." *Lerner v. Nw. Biotherapeutics*, 273 F. Supp. 3d 573, 588 (D. Md. 2017) (quotation omitted).

"The complaint's basic problem is that the facts it alleges do not contradict [Marriott's] public disclosures." *Teachers' Ret. Sys. of La. v. Hunter*, 477 F.3d 162, 182 (4th Cir. 2007).[6]

A. Defendants' Affirmative Statements Are True And Inactionable.

1. Statements About Due Diligence And Integration

Plaintiff challenges statements regarding Marriott's due diligence and progress on integrating Starwood, ¶¶ 442–54, 464–82, 489–91, 501–02, 526–27, 543–47, 574–83, but fails to plead that those statements were false.

i) Due Diligence. Plaintiff labels Marriott's high-level updates regarding its due diligence for the Acquisition "false and misleading" because supposedly "Starwood's IT systems were

[6] Because Defendant's statements are consistent with the facts, Plaintiff contrasts the facts with supposedly "false impression[s]" of Plaintiff's invention. ¶¶ 446, 451, 454, 469, 472, 482, 491, 500, 512, 521, 547, 559, 566, 573, 576. This is a straw man argument, and it lacks merit. The securities laws make Defendants accountable for *their* statements, not "impressions" made up by litigants. *See, e.g.*, *Detroit Gen. Ret. Sys. v. Medtronic, Inc.*, 621 F.3d 800, 806 (8th Cir. 20210); *Xiaojiao Lu v. Align Tech., Inc.*, 417 F. Supp. 3d 1266, 1276–77 (N.D. Cal. 2019); *Jui-Yang Hong v. Extreme Networks, Inc.*, 2017 WL 1508991, at *15 (N.D. Cal. Apr. 27, 2017).

severely vulnerable" and "[a]n adequate merger due diligence process would have easily revealed these glaring deficiencies." ¶¶ 450, 468, 475, 479. But Defendants made *no* representations regarding due diligence on Starwood's IT systems in particular. And the Complaint pleads no facts suggesting that the Company did not perform every one of the steps it actually mentioned in statements about its due diligence, such as "consult[ing] with Marriott's senior management, legal advisors, financial advisors, and other advisors," "review[ing] a significant amount of information," or conducting "extensive" diligence overall. ¶¶ 123, 448, 464-67, 474. Plaintiff's failure to "allege that [Marriott] did not, in fact, take each" of these "specific diligence steps" compels dismissal of these claims. *City of Austin Police Ret. Sys. v. Kinross Gold Corp.*, 957 F. Supp. 2d 277, 298 (S.D.N.Y. 2013). Indeed, accepting Plaintiff's confidential witness allegations as true, it is undisputed "that the due diligence process was extremely detailed." ¶ 175.

Plaintiff's suggestion that "even the most cursory due diligence on Starwood's Systems" would have revealed that "critical safety standards were violated," ¶ 41, cannot help Plaintiff avoid dismissal. "Plaintiffs do not get the benefit of 20/20 hindsight." *In re Under Armour Sec. Litig.*, 342 F. Supp. 3d 658, 677 (D. Md. 2018). After-the-fact speculation about what Plaintiff believes Marriott's due diligence should have discovered cannot establish falsity, particularly where Marriott made no representations about its "diligence on Starwood's Systems," let alone a representation that it applied any particular standards to such diligence. Simply put, "the reasons Plaintiffs offer as to why many of the statements are false or misleading bear no connection to the substance of the statements." *Veal v. LendingClub Corp.*, 423 F. Supp. 3d 785, 807 (N.D. Cal. 2019).

ii) Integration of Starwood. The Complaint likewise alleges no facts refuting the accuracy of any statements regarding the integration process, including that Marriott conducted "extensive" or "exhaustive" integration planning, the companies were "working intensely" or "diligently" to

ensure a smooth transition, and the teams were working in an effort to ensure the integration succeeded with minimal business disruption. ¶¶ 442–44, 452, 464, 466, 467, 470, 474, 476, 478, 480, 489, 501, 545. To the contrary, the Complaint confirms that these statements were true. It acknowledges that, by April 2016, "Starwood and Marriott integration teams had met approximately 150 times," ¶ 147, *see also* ¶ 478, and that, "as part of the company's integration efforts, Marriott conducted an assessment of the legacy Starwood IT systems," ¶ 139.[7]

Plaintiff also claims that Defendants falsely described the integration as "on track" or in the "home stretch," ¶¶ 480, 526, 543, 578, 580, 582. But the Complaint offers no criteria for assessing what amount of progress would have qualified as "on track," and Plaintiff cannot plead falsity without explaining the reason why the statements were false. *See OFI Asset Mgmt. v. Cooper Tire & Rubber*, 834 F.3d 481, 500 n.19 (3d Cir. 2016) (rejecting "general allegation that [company] 'falsely and misleadingly assured investors that the Merger was on track'"). Moreover, the Complaint admits "that Marriott management's primary focus was getting the loyalty programs integrated in time for the closing of the [acquisition]" and this goal was "completed on time." ¶ 216.

2. Statements of Optimism About The Acquisition

Plaintiff disparages Defendants' expressions of optimism about the Acquisition, including the Company's belief that "the prospects for the combined company are favorable," ¶ 449, and that it was "even more convinced of the tremendous opportunity presented by this merger," ¶ 465; *see*

[7] The Complaint decries statements made by Marriott's CIO, Mr. Hoffmeister, in an interview with a trade publication called *Hospitality Upgrade*, which obviously was not directed at investors. ¶ 545–46 (quoting http://mag.hospitalityupgrade.com/publication/?i=468555&article_id=2983805&view=articleBrowser&ver=html5). In response to a question about the integration process, Mr. Hoffmeister responded that the Company has "a lot of work ahead still" and is trying "to get the best of both worlds wherever possible" in merging Marriott's and legacy Starwood's computer systems. ¶ 545. Although these statements concern IT generally, they have nothing to do with cybersecurity, and there is no allegation that Marriott had any intention other than to utilize the best aspects of each company's systems when it could.

also ¶¶ 450–54, 458–59, 464–69, 473–75, 483–84, 489–93, 503–04, 513–14, 519–21, 528–29, 536–38, 551–52, 557–59, 564–66, 584–86. These claims fail for three, independent reasons.

First, these "'[s]oft, "puffing" statements'" are "mere expressions of optimism . . . not worded as guarantees" that "lack materiality"; therefore, they are nonactionable. *Raab v. Gen. Physics Corp.*, 4 F.3d 286, 289–90 (4th Cir. 1993); *see also Local IBEW Union No. 58 Pension Tr. Fund & Annuity Fund v. Royal Bank of Scot. Grp., PLC*, 783 F.3d 383, 392 (2d Cir. 2015) (statements that "[company's] positive view . . . has been confirmed" and "acquisition . . . has rarely seemed more attractive" were "inactionable puffery").

Second, these optimistic statements are opinions that cannot be false unless (1) the speaker does not "actually hold[] the stated belief," (2) the statements "contain embedded statements of untrue facts," or (3) there are omitted facts that "conflict with what a reasonable investor . . . would take from the statement itself." *Omnicare Inc. v. Laborers Dist. Council Const. Indus. Pension Fund*, 575 U.S. 175, 176 (2015). "[A] sincere statement of pure opinion is not an 'untrue statement of material fact,' regardless whether an investor can ultimately prove the belief wrong." *Id.* at 186. Plaintiff does not plead falsity under this standard. The Complaint is devoid of allegations that Defendants did not believe the Acquisition offered opportunities. While Plaintiff recycles the same laundry list of purported "glaring deficiencies" in Starwood's IT systems, *see, e.g.*, ¶¶ 468, 475, "[s]imply juxtaposing aspirational public statements with paragraphs referring to [Starwood's] internal issues does not properly allege the falsity of the statements," *Lomingkit v. Apollo Educ. Grp. Inc.*, 2017 WL 633148, at *14 (D. Ariz. Feb. 16, 2017). There are no specific allegations that Defendants knew about the supposed deficiencies when they expressed optimistic opinions or that they would not have been optimistic about the transaction as a whole even if they had known about them. The Complaint also alleges no untrue facts imbedded in Defendants' opinions.

Even viewed (impermissibly) in hindsight, the Complaint shows no daylight between Defendants' statements and the facts. That Starwood was attacked by cybercriminals by no means suggests that the benefits of the Acquisition were not compelling or that the business prospects for the combined company were unfavorable. Indeed, even on the day that Marriott disclosed the data security incident (before the rebound that immediately followed), its stock price traded at 158% of its price on the day of trading before Marriott announced the Acquisition.[8]

Third, the PSLRA forecloses liability for predictive statements, called "forward-looking statements," when they are accompanied by meaningful cautionary language. *See*, *e.g.*, *In re Constellation Energy Grp., Inc. Sec. Litig.,* 738 F. Supp. 2d 614, 625 (D. Md. 2010). This protection applies even if the predictions prove to be incorrect in hindsight. *See, e.g.*, *Fort Worth Emp'rs. Ret. Fund v. Biovail Corp.*, 615 F. Supp. 2d 218, 231 (S.D.N.Y. 2009). All of Defendants' optimistic statements were clearly forward-looking and accompanied by meaningful cautionary language.[9]

3. Risk Factor Disclosures

Plaintiff's attempt to cast the Company's "risk factor" disclosures regarding cybersecurity and the Acquisition as misstatements also fails. *See* ¶¶ 458–61, 483–86, 492–95, 503–06, 513–16, 519–23, 528–31, 537–40, 551–54, 557–61, 564–68, 585–88. Risk factor disclosures, which the SEC instructs companies to include in their public filings, are prospective "discussion[s] of the most significant factors that make an investment in the [specific company] risky." 7 C.F.R. § 229.105 (Reg. S-K, Item 105). In compliance with this instruction, Marriott consistently disclosed, among other things, that "[c]yber-attacks could have a disruptive effect on our business," "the integration

[8] *Compare* ¶ 39, *with* Yahoo! Finance, Marriott Int'l, Inc., https://finance.yahoo.com/quote/MAR/history?period1=1447372800&period2=1543795200&interval=1d&filter=history&frequency=1d (last visited Sept. 8, 2020).

[9] *See* Ex. A (Forward-Looking Statements Accompanied by Meaningful Cautionary Language). These claims also fail under the "bespeaks caution" doctrine, which "operates in a similar fashion and protects forward-looking statements accompanied by adequate cautionary language from being actionable." *In re QLT Inc. Sec. Litig.*, 312 F. Supp. 2d 526, 532 (S.D.N.Y. 2004).

process is subject to a number of uncertainties," and there may be difficulty "harmonizing our different reservations and other systems." *E.g.*, ¶¶ 503, 528, 530.

The Complaint claims the risk factors were "false and misleading" for "fail[ing] to disclose critical facts relevant to these risks that ***existed at the time***, including the vulnerability of the customer data and that the Data Breach was currently ongoing." ¶¶ 459, 461, 484, 486, 493, 495, 504, 506, 514, 516, 520, 523, 529, 531, 538, 540, 552, 554, 558, 561, 565, 568, 586, 588. Plaintiff's contention that Defendants had to disclose that the attack was "ongoing" before they even learned it occurred is nonsensical. *See* ¶ 31 (alleging Marriott "finally discovered" the attack in "September 2018").

In any event, risk factors disclosures are "not actionable to the extent plaintiffs contend defendants should have disclosed risk factors 'are' affecting financial results rather than 'may' affect financial results" because they are "not meant to educate investors on what harms are currently affecting the company." *In re ChannelAdvisor Corp. Sec. Litig.*, 2016 WL 1381772, at *5 (E.D.N.C. Apr. 6, 2016) (quoting *Bondali v. Yum! Brands, Inc.*, 620 F. App'x 483, 491 (6th Cir. 2015)), *aff'd sub nom. Dice v. ChannelAdvisor Corp.*, 671 F. App'x 111 (4th Cir. 2016). Because "[a] reasonable investor would be unlikely to infer anything regarding the ***current*** state" of Marriott's cybersecurity and "from a statement intended to educate the investor on ***future*** harms," Plaintiff's claims fail. *Bondali*, 620 F. App'x at 491 (first emphasis added).

Moreover, Plaintiff mischaracterizes Marriott's risk factor disclosures from the third quarter of 2018. ¶¶ 584–90. Plaintiff argues those disclosures were misleading because they warned only of "potential risks the Company might face as a result of the" Acquisition when Defendants already had "actual knowledge of the Data Breach." ¶¶ 585–86, 588. But the Complaint's quotation of the disclosures show that they stated, in the past tense, that "we ***have experienced cyber-attacks***, attempts to disrupt access to our systems and data, and attempts to affect the integrity of our data,"

¶ 587 (emphasis added), and "***have encountered challenges*** in harmonizing our different reservations and other systems," ¶ 585 (emphasis added). These disclosures reflected a change from the Company's risk factor disclosures in prior quarters. *See* ¶¶ 564, 567.[10]

4. Statements Regarding Marriott's Commitment To Protecting Customer Data

Plaintiff challenges statements from Marriott's SEC filings describing the Company's commitment to safeguarding the data and personal information of its customers and employees. Again, Plaintiff fails to plead more than conclusory assertions of falsity.

First, Plaintiff claims it was false for Marriott to say that its "customers and employees . . . have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information." ¶¶ 460, 485, 494, 505, 515, 522, 530, 539, 553, 560, 567, 587. This "statement is undeniably a reference to a belief as to what third parties think about the company and its products, not an assertion or guarantee by the company as to a fact." *In re Lululemon Sec. Litig.*, 14 F. Supp. 3d 553, 578 (S.D.N.Y. 2014), *aff'd*, 604 F. App'x 62 (2d Cir. 2015).

Second, the Complaint alleges no facts refuting the truth of Defendants' statements that "[t]he integrity and protection of . . . customer, employee, and company data is critical to our business." ¶¶ 456, 460, 485, 494, 505, 510, 515, 522, 530, 539, 549, 553, 560, 567, 587. There is nothing inconsistent between data being important and also vulnerable to a cyberattack. As in *Heartland*, Marriott did not say "that the company's network was immune from security breaches or that no security breach had ever occurred." 2009 WL 4798148, at *6.

[10] Plaintiff also claims that certifications Mr. Sorenson and Ms. Oberg signed under the Sarbanes-Oxley Act of 2002 ("SOX") were false and misleading because they certified the accuracy of the risk factor disclosures. *See* ¶¶ 462–63, 487–88, 496–97, 507–08, 517–18, 524–25, 532–33, 541–42, 555–56, 562–63, 569–70, 589–90. Because Plaintiff fails to plead that the risk factor disclosures were false or misleading, the SOX certification claims fail too.

Moreover, the Complaint repeatedly admits Marriott *did* view the protection of customer data as important, detailing its investments in outside experts and board proceedings at which cybersecurity was ranked as a top risk facing the Company. *See* ¶¶ 21–24. Plaintiff also admits Marriott dedicated substantial resources to cybersecurity, including "perform[ing] two different audits of [its] IT systems annually," and taking care to "pull resources from other teams to assist with IT security" following the Acquisition. ¶¶ 207, 214; *see also* ¶ 164 (alleging that Starwood had thousands of IT contractors "on-site" where "IT and security projects were implemented"). These allegations "do not support an inference that [Marriott] did not make serious efforts to protect its computer network from security breaches." *In re Heartland*, 2009 WL 4798148, at *6.

Finally, Marriott's general commitments to safeguarding data are immaterial under the securities laws. *See, e.g.*, ¶¶ 456, 510, 549 ("the integrity and protection of customer, employee, and company data is critical to us"). Numerous courts have recognized that "'commitment' statements are inactionable puffery." *In re Extreme Networks, Inc. Sec. Litig.*, 2018 WL 1411129, at *23 (N.D. Cal. Mar. 21, 2018); *In re Alphabet*, 2020 WL 2564635, at *4 (finding "generalized statements" about "Alphabet's general commitment to . . . protection of [user] data . . . inactionable puffery"). "In other words, '[n]o investor would take such statements seriously in assessing a potential investment, for the simple fact that almost every [similar company] makes these statements.'" *In re Constellation Energy Grp., Inc. Sec. Litig.*, 2012 WL 1067651, at *12 (D. Md. Mar. 28, 2012).

5. Privacy Statements

The Complaint challenges snippets from the customer-facing Privacy Statements Marriott and legacy Starwood posted on their websites, but they are not actionable. *See* ¶¶ 498–500, 534–35, 571–73. Two of these statements told customers "[w]e seek to use reasonable organizational, technical and administrative measures to protect Personal Information within our organization," ¶¶ 498, 571, and the third that "we safeguard your information using appropriate administrative,

procedural and technical safeguards," ¶ 534. Two of the statements also noted that Marriott seeks to comply with or have certified to certain privacy principles or frameworks. ¶¶ 534, 571. Plaintiff claims these statements were false and misleading because "Starwood's IT systems . . . were severely vulnerable" and the statements "gave investors a false impression" about their operation "in accordance with relevant requirements, standards, and best practices." ¶¶ 499–500; *see also* ¶¶ 535, 572–73.

Plaintiff's contentions fail for numerous reasons. First, there is no allegation that Marriott did not seek to comply with privacy standards or use security measures it believed were "reasonable." Second, the Complaint does not allege that Marriott claimed to use any particular security measure that it did not in fact use. Indeed, the Starwood privacy statement enumerated specific measures that were in place, *see* ¶ 534, and the use of those measures is undisputed. Third, each of the statements candidly cautioned customers that data security could never be guaranteed. ¶¶ 498, 571 ("[N]o data transmission or storage system can be guaranteed to be 100% secure."); ¶ 534 ("'[G]uaranteed security' does not exist either on or off the Internet."). That caution is exactly the opposite of the "impression" the Complaint misleadingly ascribes to these statements. *See In re Intel*, 2019 WL 1427660, at *10 ("[R]easonable investors understand that a 'vulnerability-resistant' product is not guaranteed to be immune from any and all security issues."). Fourth, there is no allegation that the Individual Defendants played any role in drafting these statements or had any cause to believe they were incorrect. Fifth, Plaintiff does not allege who prepared these statements or that those persons had any knowledge of the supposed security deficiencies. Thus, none of the Privacy Statements challenged by the Complaint is actionable.

More fundamentally, these statements were not made "in connection with" the purchase or sale of a security, as required under Section 10(b), because they were entirely consumer-facing and

not "'disseminated to the public in a medium upon which a reasonable investor would rely.'" *SEC v. Pirate Inv'r LLC*, 580 F.3d 233, 244 (4th Cir. 2009) (citation omitted). As the Ninth Circuit reasoned in analogous circumstances, these statements "***might*** have some probative value in an action based on consumer protection laws, but they have none in a case alleging investor fraud." *In re LifeLock, Inc. Sec. Litig.*, 690 F. App'x 947, 954 (9th Cir. 2017).

B. Defendants Omitted No Required Disclosure.

Although Plaintiff contends that this case is "primarily predicated upon omissions," ¶ 645, the Complaint fails to allege that Defendants omitted any fact they had a legal duty to disclose, ¶¶ 442–590. Therefore, Plaintiff's omissions claims fail as a matter of law.

Section 10(b) and Rule 10b–5(b) "do not create an affirmative duty to disclose any and all material information." *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011) (quoting 17 C.F.R. § 240.10b–5(b)). "Even with respect to information that a reasonable investor might consider material, companies can control what they have to disclose . . . by controlling what they say to the market." *Id*. at 45. "Disclosure is required . . . only when necessary 'to make statements made, in the light of the circumstances under which they were made, not misleading.'" *Lerner*, 273 F. Supp. at 588 (citing *Matrixx*, 563 U.S. at 44); *see also In re Heartland*, 2009 WL 4798148, at *6. The PSLRA confirms this principle, providing that plaintiffs can plead an actionable omission only by alleging that a defendant "omitted to state a material fact necessary" to make an affirmative statement "not misleading." 15 U.S.C. § 78u–4(b)(1)(B). Moreover, plaintiffs must "specify each" affirmative statement alleged to be misleading to due to the omission. *Id*.

Plaintiff fails to plead that Defendants omitted any facts necessary to make their affirmative statements not misleading. Plaintiff complains that Defendants omitted to announce that "Starwood's IT systems were severely vulnerable" and "failed to share" purported "deficiencies" with Starwood's systems. *E.g.*, ¶¶ 445, 450, 453, 468, 471, 481, 490, 499, 511, 520, 546, 558, 565,

572, 575. But Defendants had no duty to denounce the Company's data security measures publicly, potentially inviting attacks, because they made no affirmative representations about those measures that were deceptively incomplete. *See, e.g.*, *In re Intel*, 2019 WL 1427660, at *13 n.17 (finding no "duty to disclose" security vulnerabilities because "none of defendants' statements were materially misleading"); *Irving Firemen's Relief & Ret. Fund v. Uber Techs.*, 2018 WL 4181954, at *5 (N.D. Cal. Aug. 31, 2018) (holding there was no "duty to disclose [Plaintiff's] 'laundry list' of allegedly fraudulent activities that are unconnected to the actual challenged statements").

Virtually none of the challenged statements have anything to do with cybersecurity measures. For example, Defendants' updates about the "integration of business units" and efforts to "understand each other's organizations[,] structures," "assets and . . . balance sheet" were generalized and did not speak to cybersecurity. ¶¶ 452, 466, 478; *see also* ¶¶ 574, 578, 580. Nor did Defendants make representations about particular security measures in stating that the "integrity and protection of customer, employee, and company data is critical to us." *E.g.*, ¶ 510. A speaker does not become obligated to speak exhaustively about a subject merely by observing the subject's importance. *See Ong v. Chipotle Mexican Grill, Inc.*, 294 F. Supp. 3d 199, 232 (S.D.N.Y. 2018) (finding no actionable omission where defendant expressed a "commit[ment]" to food safety practices but did not disclose deviations from those practices). Although Plaintiff challenges a Global Privacy Statement that does list certain security measures Starwood employed, ¶ 534, there is no allegation that any listed measure was not fully employed, *see supra* Part II.A.5.

Plaintiff also assails Defendants for not disclosing the data security incident in its SEC filing shortly after the Company discovered there had been suspicious queries in the Starwood Guest Reservation Database. *See* ¶¶ 586, 588. But Marriott's quarterly report for the third quarter of 2018—its first regular public filing following the discovery—***did*** explicitly disclose that the

Company had been subject to "cyber-attacks, attempts to disrupt access to [its] systems and data, and attempts to affect the integrity of [its] data." ¶ 587. Plaintiff cites no legal basis for asserting that the Company was required to provide any more detail at that time, and there is none. *See, e.g.*, *In re Heartland*, 2009 WL 4798148, at *5–7.[11]

C. This Court Has Not Sustained Plaintiff's Deficient Allegations.

Plaintiff attempts to dodge its burden to plead misstatements or omissions that are actionable under the PSLRA by implying that the Court has already decided this issue in its favor. ¶¶ 296, 446, 451, 454, 469, 472, 482, 491, 500, 512, 521, 547, 559, 566, 573, 576. That argument is misleading. The Court's earlier decision concerned consumer claims under the Maryland Consumer Protection Act, which has no bearing here. ECF No. 540 at 59–62. This Court reasoned that the consumers adequately pleaded reliance on omissions about Marriott's "allegedly inadequate data security practices and the risk of a data breach" in deciding to pay for Marriott's goods and services, *id*., and entrust Marriott with their personal data, *id*. at 3.

This reasoning has no application here. First of all, this Court did not apply the heightened pleading burdens of the PSLRA in its prior decisions.[12] Moreover, Marriott's knowledge of its data security practices and risks is irrelevant here because Plaintiff does not plead that the Company told investors anything contrary to that knowledge. *See supra* Parts II.A & B. Finally, the context in this

[11] When Marriott filed this quarterly report on November 6, 2018, it was still investigating the data security incident. *See* ¶¶ 255–58. In fact, the Company did not discover the possible exposure of customer data—even in encrypted form—until two weeks later, on November 19, 2018. ¶ 259.

[12] Plaintiff's contention that the consumer plaintiffs pleaded that Marriott ***knew*** about inadequate cybersecurity practices under Rule 9(b) also is misleading. *See, e.g.*, ¶¶ 296, 446. Rule 9(b) concerns the circumstances of misstatements, not knowledge or intent. As the Court explained, Rule 9(b) requires plaintiffs to allege "the time, place, and contents of . . . false representations" and is applied "less strictly" to omissions claims. ECF No. 540 at 60–61 (citations omitted). Thus, the Court reasoned that the consumers sufficiently alleged that the omitted information would have been important in their decision to purchase Marriott's goods and services. *Id*. at 61 (citations omitted). The Court had no occasion to decide whether the consumers had also pleaded Marriott's *knowledge* with particularity under Rule 9(b). In any event, the PSLRA's unique requirements for pleading scienter far exceed those of Rule 9(b), including by requiring the balancing of inferences. *Hunter*, 477 F.3d at 184.

case is entirely different. What would be material to consumers who were deciding whether to provide their personal data has no bearing on what Marriott had a legal duty to disclose to investors who were deciding whether to buy stock. The Court should reject Plaintiff's characterization of its rulings and evaluate the sufficiency of Plaintiff's claims under the standards applicable here.

III. THE COMPLAINT FAILS TO PLEAD A STRONG AND COMPELLING INFERENCE OF SCIENTER.

The PSLRA requires that a securities complaint "shall, with respect to each act or omission alleged to violate this chapter, state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." 15 U.S.C. § 78u-4(b)(2)(A). As construed by the Fourth Circuit, pleading the "required state of mind" means alleging "a strong inference that [Defendants] intentionally or recklessly deceived, manipulated, or defrauded investors." *Maguire Fin., LP v. PowerSecure Int'l, Inc.*, 876 F.3d 541, 547 (4th Cir. 2017). "[A]n inference of scienter can only be strong—and compelling, and powerful—when it is weighed against the opposing inferences that may be drawn from the facts in their entirety." *Cozzarelli*, 549 F.3d at 624. After comparing "the malicious and innocent inferences," courts may "only allow the complaint to survive a motion to dismiss if the malicious inference is at least as compelling as any opposing innocent inference." *Yates*, 744 F.3d at 885 (quotation marks and citation omitted).[13]

Here, the Complaint does not attempt to plead scienter as to ***each*** alleged misstatement, as the PSLRA requires, and its generalized scienter allegations are wholly irrelevant. They center on whether Defendants "knew, or were at least severely reckless in not knowing about . . . deficiencies in Starwood's IT systems" and Marriott's supposed failure to "address" them. ¶ 592. Because the

[13] The Supreme Court has not ruled on whether reckless deceit constitutes scienter. Although the Fourth Circuit has, Defendants maintain that only intentional fraud is actionable and reserve the right to advance that argument in the appropriate appellate forum.

statements Plaintiff challenges do not disclaim such deficiencies or assure investors they have been "addressed," what Defendants knew about these topics is entirely beside the point.

What is relevant and dispositive is that there are no allegations supporting the inference that Defendants subjectively believed that any disputed statement would lead investors to conclude that Marriott had neutralized every risk associated with the Acquisition or—unlike every other company in the world—was invulnerable to cyberattacks. In fact, the Complaint is replete with allegations that support the opposing inference that Defendants believed their statements were true and would not mislead investors. Thus, even if any of the challenged statements could be deemed to be inaccurate, this case must be dismissed. *See, e.g.*, *Maguire Fin.*, 876 F.3d at 548 (holding that even "[a]n inference that an executive had enough knowledge to be aware that he was making an inaccurate statement . . . does not necessarily suggest an intent to mislead" investors).

A. The Confidential Witness Allegations Fail To Plead Scienter.

The Complaint expends 70 paragraphs on summarizing the opinions of unidentified confidential witnesses, to whom it refers as "CWs." ¶¶ 13–15, 19–20, 64–70, 152–71, 175–86, 191–213, 592–97. For several reasons, these allegations are deficient.

First, the CW allegations have nothing to do with the truth of any Defendant's representations to investors. Without exception, the CWs' opinions concern the sufficiency of the Company's cybersecurity measures. *See, e.g.*, ¶¶ 151–73 ("Oracle Deficiencies Lead to Security Vulnerabilities" and "Starwood's Security Deficiencies Expose Valuable Data"). That is not what the securities laws concern, and the CW allegations can be brushed aside on this ground alone.

Second, "'[n]ot one of Plaintiffs' confidential witnesses provides any information about how . . . each Defendant knew of the purported fraud.'" *In re Acterna Corp. Sec. Litig.*, 378 F. Supp. 2d 561, 574 (D. Md. 2005) (quotation omitted). CW 2 and CW 3 never worked at Marriott, ¶¶ 65–66,

and could not have any personal knowledge about the state of mind of the management or directors of Marriott. *See Shah v. GenVec, Inc.*, 2013 WL 5348133, at *5 n.7 (D. Md. Sept. 20, 2013) (CW whose "employment was terminated in January 2009 . . . could have had no credible basis of knowledge as to events occurring internally at GenVec in 2010").

The claims attributed to the remaining CWs fare no better. The Complaint does not allege that any CW ever interacted directly with any Individual Defendant, and thus Plaintiff's suggestion that the CWs "knew what the Defendants knew or recklessly disregarded" "defies logic." *In re Coventry Healthcare, Inc. Sec. Litig.,* 2011 WL 1230998, at *6 (D. Md. Mar. 30, 2011); *see also In re Heartland*, 2009 WL 4798148, at *8 ("[E]ven if there were a handful of lower-level employees who were worried about ongoing problems created by the attack, there is nothing in the Complaint that supports an inference that these concerns were ever relayed to any of the Defendants."). Although CW 5 allegedly "ultimately" reported to Mr. Hoffmeister, ¶ 68, CW 5 is not alleged to have communicated his views to Mr. Hoffmeister on any relevant topic. Therefore, his opinions are of no moment. *See In re Synchronoss Techs., Inc. Sec. Litig.*, 2019 WL 2849933, at *10 (D.N.J. July 2, 2019) ("CW3 [is n]ever alleged to have had any direct contact with [defendant], which is unsurprising given that CW3 reported only 'indirectly'" to her.).

Third, the allegations attributed to CW 6 are rife with unreliable hearsay, speculation, and generalizations. *Compare e.g.*, ¶¶ 191, 194, 217, *with Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 996 (9th Cir. 2009) (finding "conclusory assertions" and "unreliable hearsay" "not sufficient to raise a strong inference of scienter").

B. The Complaint Fails To Cite Any Contemporaneous Documents That Support An Inference of Scienter.

The Complaint liberally cites contemporaneous documents and information discussed in other lawsuits, but none of it supports an inference of scienter under the securities laws.

For example, the Complaint cites a "Marriott internal report" from 2016, two PwC "Starwood Cybersecurity Assessments" from 2017, and a report from Protiviti in 2018, all of which purportedly show deficiencies in "Starwood's system." ¶¶ 608–09. But the Complaint does not plead that any of these reports cast doubt on the truth of the Defendant's statements or contained information that was required to be disclosed under the securities laws. Nor does the Complaint plead, except in the vaguest terms, the Individual Defendants knew about or agreed with these reports: "Missing are allegations linking specific reports and their contents to the executives." *Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc.*, 759 F.3d 1051, 1063 (9th Cir. 2014). Although CW 1 allegedly "said that everyone was made aware of the findings from the third audit, including the Board, Defendant Sorensen and Defendant Hoffmeister," ¶ 215, this assertion cannot be credited because Plaintiff fails "to allege facts demonstrating that the [CWs] consulted were in a position to know what management knew," *Knollenberg v. Harmonic, Inc.*, 152 F. App'x 674, 681 (9th Cir. 2005). Furthermore, the point of conducting penetration tests is to find vulnerabilities proactively. So even if Defendants knew their experts had done so, that knowledge would support the inference that they believed Marriott was working to harden its cybersecurity, not the opposite. Such knowledge certainly would not suggest that the Company was misleading investors about anything.

Plaintiff also relies on certain "past cybersecurity incidents," *see* ¶ 611–14, but Plaintiff cannot manufacture a "red flag" out of Starwood's "RAM-scraper malware breach" in 2015, ¶¶ 361–62, or other "breaches in the hospitality industry in 2015 and 2016," ¶ 612. All of these events were "public knowledge, diluting any significant inference of scienter that can be drawn therefrom." *Knurr v. Orbital ATK Inc.*, 272 F. Supp. 3d 784, 802–03 (E.D. Va. 2017). Furthermore, Mr. Sorenson's Senate testimony, which the Complaint incorporates by reference, ¶ 44, reflects that Starwood's prior breach "was totally unrelated to the reservation system breach" that is the subject

of this lawsuit, *see* Examining Private Sector Data Breaches: Hearing Before the Permanent Subcomm. on Investigations of S. Comm. on Homeland Sec. & Gov't Affairs, 116th Cong. 33–34 (2019), www.hsdl.org/?abstract&did=828236.

The Complaint assumes that other documents the Defendants might have reviewed provided them "knowledge of facts or access to information contradicting their public statements," but no contradictions are pleaded. *In re Constellation*, 2012 WL 1067651, at *6. For example, the Complaint cites board materials showing that Marriott's management advised the Audit Committee that cybersecurity was "the number one risk facing" the company in 2016, ¶ 604, but that conclusion underscores management's attention to this issue and is not contrary to Marriott's public disclosures, which repeatedly cautioned that cybersecurity was a risk, *see, e.g.*, ¶¶ 485, 494. The Complaint fails to match the disputed statements with contradictory facts the Defendants received, and thus lacks "particular allegations which strongly imply Defendants' *contemporaneous* knowledge that the statement was false when made." *In re Under Armour*, 342 F. Supp. 3d at 691 (citation omitted).

Defendants' statements about the Acquisition provide no support for an inference of scienter either. *See* ¶¶ 615–16. Plaintiff caricatures the Acquisition as being pursued "primarily to access Starwood's customers and their data," and avers that Defendants were thus required to conduct due diligence to "secure their investment." ¶ 615. This is an absurd portrayal of Marriott's acquisition of ***thousands*** of hotel properties, and there is no allegation that Defendants failed to conduct due diligence. To the contrary, accepting the CW allegations as true, the Complaint admits "that the due diligence process was extremely detailed," ¶ 175, and Plaintiff's quotations of Messrs. Hoffmeister and Flaherty confirm that Marriott analyzed Starwood's systems, before and after the Acquisition, ¶ 616. In any event, what Defendants knew about Marriott's due diligence is irrelevant to scienter because they are not alleged to have said anything inconsistent with that knowledge.

C. Assessments Of Marriott's Cybersecurity After The Attack Was Detected Have No Bearing On Scienter.

The Complaint places heavy reliance on the PFI Report that was "commissioned after the Data Breach." ¶ 599. But the PFI Report has no bearing on scienter. First of all, it has nothing to do with Defendants' representations to investors; it merely "memorialized" the "forensic investigation into the causes" of the cybersecurity incident. ¶ 40. Defendants never represented that there was nothing more that could be done to protect Marriott's data at any cost or that Marriott was immune to the attacks that plague all businesses and government entities across the globe. And there are no factual allegations that Defendants tried to trick anyone into believing that.

Furthermore, the PFI Report contains a technical analysis of the causes of the data security incident but no information about what any ***Defendant*** knew about cybersecurity. *See* ¶¶ 330–80 (summarizing report without referencing any Individual Defendant). The PFI Report certainly does not address any Defendants' knowledge at the time any challenged statement was made, as it was issued on May 6, 2019—almost six months ***after*** the end of the class period. *See* ¶ 1 & Compl. Ex. A. Plaintiff's reliance on assessments performed half a year after the relevant period "constitute fraud by hindsight and do not satisfy [Plaintiff's] burden under the PSLRA to adequately plead fraud." *In re E.Spire Commc'ns, Inc. Sec. Litig.*, 127 F. Supp. 2d 734, 748 (D. Md. 2001).

Moreover, Plaintiff's assertion that "Marriott would have uncovered further evidence that Starwood's systems were extremely vulnerable" if Defendants had "conducted proper due diligence," ¶ 332, is not a particularized allegation of scienter, but speculation about what might have occurred if hypothetical defendants took hypothetical steps. The question here is whether Plaintiff pleaded that ***these*** Defendants, based on what they knew, were reckless or deliberately deceitful in their representations to investors. The clear answer is no. *See Shields v. Citytrust Bacorp, Inc.*, 25

F.3d 1124, 1129–30 (2d Cir. 1994) (rejecting claims that "defendants should have been more alert and more skeptical").

The Complaint's assertions that Marriott violated various cybersecurity and corporate governance standards likewise do not salvage its deficient scienter allegations. The Complaint does not allege that Defendants knowingly made any misrepresentations about these standards. *See* ¶¶ 598–602. For example, the Complaint invokes "the principles laid out in the COSO [and] . . . EU-US Privacy Shield" frameworks, and speculates about Marriott's supposed "failure to adhere to these standards and best practices." ¶¶ 601–02. Plaintiff does not contend that either the COSO or Privacy Shield frameworks imposed binding rules on Marriott. Indeed, Plaintiff acknowledges that they consist of "principles," ¶ 602 and admits the "COSO framework" does ***not*** prescribe "exactly which controls need to be implemented," ¶ 396. Moreover, Marriott's SEC filings make clear that it applies the COSO framework to "the Company's internal control over financial reporting," not cybersecurity. *E.g.*, Ex. B at 47. Nor is there any allegation that the FTC Act imposed any specific requirement the Company did not satisfy, much less that Defendants knew that and stated otherwise.

In any event, the occurrence of the data security incident does not show that any of these principles were violated, and conclusory allegations, in hindsight, of violations do not satisfy Plaintiff's burden to plead what each Defendant knew at the time of any challenged statement. *See, e.g.*, *Doshi v. Gen. Cable Corp.*, 823 F.3d 1032, 1043–44 (6th Cir. 2016) (speculating what defendants "would have known" had they "properly used the COSO framework" "amount[s] to impermissible fraud by hindsight"); *Fire & Police Pension Ass'n of Colo. v. Abiomed, Inc.*, 778 F.3d 228, 246 (1st Cir. 2015) ("[T]his case is not about whether or not defendants violated [federal] regulations. It concerns alleged violations of securities laws[.]").

Plaintiff's reliance on preliminary findings of the ICO likewise is misplaced. *See* ¶ 600.

These findings are non-determinative, *post hoc*, and uninformative with regard to anything Defendants knew about their statement to investors. *See In re Intel Corp. Derivative Litig.*, 621 F. Supp. 2d 165, 175 (D. Del. 2009) (declining to "place great weight on a 'preliminary' finding" that the company had infringed the European Commission Treaty).

D. The Timing Of The Announcement Of The Data Security Incident Does Not Support Any Inference Of Scienter.

Plaintiff's claim that the Board "had actual knowledge of the Data Breach more than ten weeks before Marriott informed the public," ¶ 605, permits no inference of scienter.

Plaintiff's depiction of the timeline is factually misleading. On September 8, 2018, Marriott learned only that its outside vendor received an alert indicating that there had been "suspicious queries" in Starwood's database. ¶¶ 32, 354. The Complaint makes clear that Marriott did not discover that customers' "personal information" was potentially accessed until November 19, 2018. ¶ 259. Even then, Marriott believed the information was encrypted and inaccessible to the attacker. *Id*. Yet, the Complaint concedes that Marriott notified interested parties of the data security incident 10 days later and publicly announced its findings on the 11th day. ¶ 262.

Plaintiff's claim also is legally misleading. The duty to notify consumers about the possible theft of their data arises under state laws that are not the subject of this lawsuit. Plaintiff seeks to represent not consumers but investors, yet fails to plead any legal duty to notify ***investors*** of the "suspicious queries" or of the potential theft of personal data any faster than Marriott did. Plaintiff also fails to plead any culpable intent with regard to the timing of Marriott's disclosures. To the contrary, the Complaint concedes that Marriott launched an immediate investigation when it learned about the suspicious queries. ¶¶ 32, 259. "Knowing enough to launch an investigation . . . is a very great distance from convincing proof of intent to deceive." *Higginbotham v. Baxter Int'l, Inc.*, 495 F.3d 753, 758 (7th Cir. 2007); *see also In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1065 (9th

Cir. 2014) (inference "that NVIDIA did not disclose because it was investigating the extent of the problem" was "more compelling"); *Knurr*, 272 F. Supp. 3d at 803 n.30 ("Taking the time necessary to get things right is both proper and lawful." (quoting *Higginbotham*, 495 F.3d at 761)).

E. Defendants' Positions Do Not Support An Inference Of Scienter.

Plaintiff formulaically contends that the Individual Defendants must have had culpable knowledge because of their roles and resulting access to information. *See* ¶¶ 621–33. Courts, however, "have routinely held that corporate executives' access to information and internal affairs is not enough to demonstrate scienter under the PSLRA." *Lerner*, 273 F. Supp. at 593; *see also In re Criimi Mae, Inc. Sec. Litig.*, 94 F. Supp. 2d 652, 661 (D. Md. 2000). Because the Complaint pleads no "additional detailed allegations" of Defendants' knowledge that contradicts their statements, it "falls short of . . . the PSLRA's particularity requirements." *Yates*, 744 F.3d at 890.

i) Audit Committee Defendants. The Complaint does not plead separate allegations for Ms. Bush and Messrs. Henderson, Lewis, Kellner, and Muñoz. Instead, it claims "The Audit Committee Defendants Acted With Scienter" collectively. ¶¶ 627–28. The Fourth Circuit has rejected this pleading tactic, because plaintiffs must "allege facts that support a 'strong inference' that ***each*** defendant acted with at least recklessness in making the false statement." *Hunter*, 477 F.3d at 184; *see also Yates*, 744 F.3d at 885 (same). As the Complaint "group[s] [the Audit Committee] Defendants together . . . when pleading knowledge or recklessness, [Plaintiff] fails to satisfy the PSLRA's heightened pleading standard." *In re Under Armour*, 342 F. Supp. 3d at 694.[14]

ii) Ms. Oberg and Messrs. Sorenson, Hoffmeister, Bauduin. Despite devoting separate subheadings to Ms. Oberg and Messrs. Sorenson, Hoffmeister, and Bauduin, *see* ¶¶ 621–26, 629–

[14] The Complaint's section titled, "Additional Allegations Supporting Scienter," largely ignores the requirement to plead scienter individually by indiscriminately addressing Defendants collectively. *Compare*, *e.g.*, ¶¶ 602, 606, 610, 614, 620, *with In re Coventry Healthcare*, 2011 WL 1230998, at *11 (refusing to infer scienter where complaint did not give the Court a precise timeline of when and how each defendant knew of errors).

33, Plaintiff does not plead any specific allegations about their intent or knowledge regarding any challenged statement. Plaintiff resorts instead to arguing "that Defendants knew or recklessly disregarded . . . errors because of their positions," but such "generic pleading . . . is insufficient to raise a strong inference of scienter." *Proter v. Medifast, Inc.*, 2013 WL 1316034, at *11–12 (D. Md. Mar. 28, 2013). Courts also regularly refuse to infer scienter merely because an officer is alleged to have been "hands[-]on," as Mr. Sorenson is alleged to have been. *Compare* ¶ 623, *with In re Mellanox Techs. Ltd. Sec. Litig.*, 2014 WL 12650991, at *19 (N.D. Cal. Mar. 31, 2014).

Plaintiff's views on what Defendants "would" or "should have" done, "based on the due diligence standards [from] the RACI matrix" and the "National Institute of Standards and Technology," add nothing. *See* ¶¶ 621, 625, 631. These standards offer general guidance on the responsibilities of various management roles, ¶¶ 413–14, 631, but absent "detailed allegations establishing the defendants' actual exposure" to relevant information, "a bare inference that a defendant must have had knowledge of the facts or must have known of the fraud given his or her position," does not support a strong inference of scienter, *Yates*, 744 F.3d at 890 (citation omitted).

Plaintiff also "allege[s] that [Mr. Sorenson and Ms. Oberg] lied when [they] certified [Marriott's SOX Certifications], but that bare allegation does not provide independent support for an inference of scienter." *Cozzarelli*, 549 F.3d 628 at n.2 (4th Cir. 2008).

F. The Duration And Scope Of The Cyberattack Against Starwood Do Not Support Any Inference Of Scienter.

Plaintiff's assertion that the data security incident was long-standing does not plead scienter. *See* ¶¶ 617–20. "[C]alling a problem 'long-standing' does not necessarily suggest that ***knowledge*** of the problem was long-standing, and knowledge is the ultimate touchstone for . . . determining recklessness." *In re Constellation*, 2012 WL 1067651, at *7. The Complaint admits that Defendants did not know about the criminal intrusion into Starwood's system until at least September 2018,

when a database security tool alerted Marriott's outside expert of a potential attack. *See, e.g.*, ¶¶ 32, 354. The length of time it took Marriott's outside expert to detect the incursion could not have caused Defendants to doubt the truth of their statements before detection.

Here, the most plausible inference to be drawn from the duration of the intrusion is that the hackers who infiltrated Starwood's system were adept at avoiding detection. This inference finds ample support in the allegations: Accenture provided "approximately 1,500 to 2,000+ workers" to implement "IT and security projects," ¶ 164; Marriott "performed two different audits of their IT systems annually," ¶ 214; yet the IBM Guardium tool did not alert Marriott to suspicious activity until September 2018, *id.* ¶ 33.

G. The Countervailing Inferences Of Innocence Are Overwhelming.

After considering the negative inferences that can be drawn from Plaintiff's largely irrelevant allegations, this Court must weigh them against the "opposing innocent inference." *Yates*, 744 F.3d at 885. Here, the innocent inferences abound.

First, Plaintiff's failure to plead any plausible fraudulent motive or insider stock sales weighs against a finding of scienter. "[A]n inability to show motive can be a relevant circumstance indicating the lack of scienter"; indeed, "there should be a negative inference regarding scienter as a result of the plaintiffs' unsuccessful attempt to demonstrate motive." *In re Acterna*, 378 F. Supp. 2d at 576–77 (quotation omitted). The Complaint is devoid of "any allegations that any individual Defendant sold any of his personally held stock at inflated prices," or had any motive to defraud investors. *Id.* Indeed, the Complaint offers no "satisfying explanation of what benefit Defendants hoped to gain by delaying disclosure of the full scope of the [data] breach by [a matter of] weeks." *PayPal*, 409 F. Supp. 3d at 859. "If there were a breach . . . , that fact could not be undone, mooted, or masked by waiting." *Id*.

Second, Marriott launched an immediate investigation when it was alerted to suspicious

inquiries. ¶ 354. These allegations "demonstrat[e] a pursuit of truth rather than reckless indifference to the truth." *Higginbotham*, 495 F.3d at 758.

Third, the Complaint admits Marriott promptly notified the FBI "of the tools used by the hackers, the timelines of the intrusion, and the forensic findings the Company and/or its third-party investigators had made." ¶ 35. To contend Marriott would embark on an illegal scheme to mislead investors at the same time it worked cooperatively with law enforcement regarding the same underlying issues is absurd. *In re Bausch Lomb, Inc. Sec. Litig.*, 592 F. Supp. 2d 323, 343 (W.D.N.Y. 2008) (scienter not pled where company "voluntarily reported the matter to the SEC").

Fourth, Defendants never suggested that Marriott was impervious to cyberattacks and could not have expected their statements to lead investors to believe otherwise. To the contrary, Marriott candidly disclosed that such attacks could adversely impact its business. *E.g.*, ¶¶ 515, 551, 567.

Because "the facts as a whole more plausibly suggest that the defendant acted innocently—or even negligently—rather than with intent or severe recklessness, the action must be dismissed." *Cozarelli*, 549 F.3d at 624.

H. The Complaint Fails To Plead Corporate Scienter.

To plead corporate scienter, Plaintiffs "must allege facts that support a strong inference of scienter with respect to at least one authorized agent" of Marriott. *Yates*, 744 F.3d at 885. Plaintiff fails to allege that any "corporate agents acted with scienter" and, thus, does not "allege scienter that can be imputed to [Marriott]." *In re Under Armour Sec. Litig.*, 409 F. Supp. 446, 463 (D. Md. 2019).

IV. THE COMPLAINT FAILS TO PLEAD LOSS CAUSATION.

The Complaint also fails to plead loss causation, "*i.e.*, a causal connection between the material misrepresentation and the loss." *Dura Pharms., Inc. v. Broudo*, 544 U.S. 336 342 (2005) (citation omitted). Loss causation must be alleged "with sufficient specificity to enable the court to evaluate whether [this] necessary causal link exists." *Hunter*, 477 F.3d at 186. This pleading

standard is "largely consonant with Fed. R. Civ. P. 9(b)'s requirement that averments of fraud be pled with particularity." *Katyle v. Penn Nat'l Gaming, Inc.*, 637 F.3d 462, 471 & n.5 (4th Cir. 2011).

Because Plaintiff premises loss causation on the drop in Marriott's stock price after disclosures that allegedly corrected misrepresentations, the Complaint must plead that the corrective disclosures "'***at least relate back to the misrepresentation*** and not to some other negative information about the company.'" *Katyle*, 637 F.3d at 473 (quotation omitted). But Plaintiff does not plead that Defendants ever stated there was no risk of a data security incident. Thus, the disclosure of the data security incident could not have had any "corrective" effect. At most, the Complaint alleges "that [Marriott]'s stock price dropped predominately as a result of announcements of disappointing" news. *Nat'l Junior Baseball League v. Pharmanet Dev. Grp. Inc.*, 720 F. Supp. 2d 517, 563 (D.N.J. 2010).

The reports the Complaint cites do not support its contention that the November 30, 2018 "share price reaction was the direct result of the market learning facts that Defendants had concealed." ¶ 643. The MarketWatch report recounts when Marriott (i) learned of the cyber-intrusion, and (ii) "decrypt[ed] the information and determine[d] the context,"[15] and describes the customer data implicated, but offers no basis to infer that Defendants had concealed that "Starwood's IT systems were severely vulnerable [or] susceptible to hacking."[16] *See id.* The Nasdaq report describes how Marriott learned "how bad [the data security incident] was" and "that hackers have had access to its systems since 2014." *See id.* This "d[oes] not even inferentially suggest that [Marriott's] prior [disclosures] were fraudulent." *Katyle*, 637 F.3d at 473–75.

---

[15] Tomi Kilgore, *Marriott's stock sinks after disclosing data breach affecting up to 500 million guests*, MarketWatch (Nov. 30, 2018), www.marketwatch.com/story/marriotts-stock-sinks-after-disclosing-data-breach-affecting-up-to-500-million-guests-2018-11-30?_sm_au_=iVVfJDHRVq4S4sNQFcVTvKQkcK8MG.

[16] William White, *MAR Stock Drops on News of Marriott Data Breach*, Nasdaq (Nov. 30, 2018), www.nasdaq.com/articles/mar-stock-drops-news-marriott-data-breach-2018-11-30.

V. THE INDIVIDUAL DEFENDANTS CANNOT BE LIABLE FOR STATEMENTS THEY DID NOT MAKE.

Only the "the person or entity with ultimate authority over the statement, including its content and whether and how to communicate it" can be held liable under Rule 10b–5. *Janus Capital Grp., Inc. v. First Derivative Traders*, 564 U.S. 135, 141–42 (2011). Plaintiff seeks to hold all Defendants liable for the vast multitude of statements disputed in the Complaint, *see* ¶¶ 442–590, but the Individual Defendants cannot be liable for statements they did not make. *See* App'x.

VI. THE COMPLAINT FAILS TO STATE A CLAIM UNDER SECTION 20(A).

Count II of the Complaint asserts a claim against all Individual Defendants under Section 20(a) of the Exchange Act. ¶¶ 664–72. Section 20(a) imposes liability on persons who "control[] any person liable under any provision of this chapter." 15 U.S.C. § 78t(a). A "claim for controlling person liability under section 20(a) must be based upon a primary violation of the securities laws." *E.g.*, *Svezzese v. Duratek, Inc.*, 67 F. App'x 169, 174 (4th Cir. 2003). Because Plaintiff has failed to establish a predicate violation of Section 10(b), Plaintiff's Section 20(a) claims should be dismissed. *See, e.g.*, *Cozzarelli*, 549 F.3d at 628 (citing *Hunter*, 477 F.3d at 188).

The Complaint also fails to plead control. *See* ¶¶ 71–77. "[W]ithout any allegation that [each Audit Committee Defendant] individually exerted control or influence over [Marriott's] day-to-day operations," their status as directors "does not suffice to support an allegation that the person is a control person." *Adams v. Kinder-Morgan, Inc.*, 340 F.3d 1083, 1108 (10th Cir. 2003). The Complaint also fails to plead that Ms. Oberg or Messrs. Bauduin or Hoffmeister "had the requisite power to directly or indirectly control or influence the specific corporate policy which resulted in the primary liability" alleged by Plaintiff. *In re Constellation*, 738 F. Supp. 2d at 639.

CONCLUSION

The Complaint should be dismissed with prejudice.

Respectfully submitted,

Dated: September 8, 2020

/s/ Jason J. Mendro

Jason J. Mendro (Bar No. 17609)
Jeffrey S. Rosenberg (Bar No. 16736)
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036
Telephone: (202) 955-8500
Facsimile: (202) 530-9550
jmendro@gibsondunn.com
jsrosenberg@gibsondunn.com

Adam H. Offenhartz (pro hac vice)
Laura K. O'Boyle (pro hac vice)
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166
Telephone: (212) 351-4000
Fax: (212) 315-4036
aoffenhartz@gibsondunn.com
loboyle@gibsondunn.com

Attorneys for Defendants

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 8th day of September 2020, I caused the foregoing Memorandum in Support of Defendants' Motion to Dismiss the Third Amended Class Action Complaint to be filed with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the counsel of record in this matter who are registered on the CM/ECF system.

/s/ Jason J. Mendro
Jason J. Mendro (Bar No. 17609)
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036
Telephone: (202) 955-8500
Facsimile: (202) 530-9550
jmendro@gibsondunn.com

Attorney for Defendants